EXHIBIT F

Declaration of William W. Fick, Esq.

Declaration of William W. Fick, Esq.

I, William W. Fick, state as follows:

1. I submit this declaration in support of the Defendant's Motion for Continuance. Specifically, I submit this declaration to explain the challenges posed by the number, nature, and content of the seized electronic devices and storage media produced by the government in discovery.

2. I am an attorney licensed to practice law in the Commonwealth of Massachusetts, employed as an Assistant Federal Public Defender, and appointed as one of the counsel of record to represent defendant Dzhokhar Tsarnaev.

3. This declaration is based on my own personal knowledge, review of documents, review of derivative evidence extracted from electronic devices, discussions with other members of the defense team who are directly involved in the forensic processing and review of the electronic devices and storage media, as well as discussions with employees of Federal Defender Organizations who provide consultation nationally on issues concerning forensic review of electronic evidence.

4. To date, the government has produced the contents of approximately 30 electronic devices[1] seized from locations connected to Mr. Tsarnaev and his brother

[1] Even at this stage of the case I still use the word "approximately" because of the often-ambiguous and disorganized manner in which some of these materials have been produced. It is not always obvious, without considerable examination, what (whose) electronic device is contained in a particular file or set of files. It appears, moreover, that certain devices have been produced repeatedly in different forms at different times. The resulting confusion is compounded because, we have seen, a single device sometimes has turned out to have more than one FBI-assigned evidence identification number and/or more than one USAO-assigned bates number (or bates range). The total of 30 is the

(thought to have been used principally by them), as well as from individuals who are immediate family members, friends, and associates of Mr. Tsarnaev and his brother.[2] The 30 devices include 7 computers, 10 data storage devices (*e.g.*, USB thumb drives and/or external hard drives), and 13 cellular telephones. Of these devices, two of the computers (belonging to Matanov and Tazhayakov, each of whom is charged in a separate related case and whose computers are very likely to contain substantial relevant evidence) and 5 of the cellular phones were produced in or after June 2014. Further, in addition to the items already included in the 30-device total, the government on August 15, 2014 produced some number of electronic devices belonging to Mr. Tsarnaev's sisters and Matanov. The defense has not yet been able to complete initial processing of these materials; therefore, I cannot now specify how many devices belonging to whom were in this latest production.

5. As the Supreme Court recently recognized:

> The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.
> . . . .

---

current best estimate, excluding duplicates, of the number of distinct seized devices and storage media actually produced by the government to date.

[2] The defense has reason to believe that the government seized a considerably larger number of electronic devices in connection with its investigation than it has produced to the defense so far, including devices seized from important individuals who were close to one or both of the brothers, *e.g.*, Ibragim Todashev, who was shot and killed by the FBI during questioning shortly after he purportedly confessed to participating, with Tamerlan Tsarnaev, in the September 2011 Waltham triple homicide.

> The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information — an address, a note, a prescription, a bank statement, a video — that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier.

Riley v. California, 134 S. Ct. 2473, 2489 (2014). In comparison to a cell phone, an actual computer or data storage device (such as a USB thumb drive or external hard drive) typically contains even more extensive information that can help to illuminate the "sum of an individual's private life."

6. The government has alleged in the indictment that certain files found on seized electronic media demonstrate Mr. Tsarnaev's interest in radical Islamic ideology and provide the motive for the Boston Marathon bombing and the other crimes that followed.

7. In its August 1expert disclosure letter, the government indicated that forensic computer examiners will testify concerning unspecified data extracted from various devices, and will further opine about the timing of certain digital activity (*e.g.*, file creation and access) as well as inferences about who was using a particular device at a particular time. If and when the government discloses the actual substance of this prospective testimony, the defense will need to verify the government's data and the inferences its witnesses seek to draw from it. As described below, this will be a time-consuming and painstaking process.

8. Apart from the government's use of evidence derived from seized devices that it deems to have evidentiary significance, the defense must conduct its own comprehensive review of the devices in order to place the government's anticipated proof in context and to ensure that a complete picture is presented to the jury.

9. Electronic devices used by Mr. Tsarnaev, his brother, and their family, friends, and associates provide an enormous trove of information that shed light on the activities, interests, and interactions with others of Tamerlan and Dzhokhar in the years leading up to the Boston Marathon bombing. In particular, analysis of evidence derived from the devices will help to illustrate the developing life trajectories, motivations, external influences, and relative roles of Dzhokhar and Tamerlan over time. Such evidence will likely play a critical role in the jury's determination not only concerning guilt but also, in the event of a guilty verdict, appropriate punishment.

10. Below, I set forth the basic methodology that must be employed to reliably examine different types of devices, with examples drawn from the evidence in the case to illustrate the volume of information some of the particular challenges to review. I also set forth the basic methodology that must be employed to trace the provenance of certain files that appear to be have been transferred or copied among multiple devices.

Computers

11. With regard to computers, two primary software tools are commonly used to perform forensic examinations and to extract relevant evidence: Internet Evidence Finder (IEF) and Forensic Toolkit (FTK).

12. **Internet Evidence Finder** is a software tool that identifies and extracts "artifacts" of internet-related activity on a device such as web browsing traces (links, cookies, referrer links, partial links), email remnants, Skype activity, cell phone backups, text messages, twitter remnants, Facebook remnants, and internet chat remnants.

13. Once IEF identifies artifacts, they must be reviewed manually, one-by-one, for potential relevance. The universe of potentially relevant information is then provided to other defense team members (*e.g.*, a mitigation specialist and/or attorney) or expert witnesses for further review and integration into the defense case preparation.

14. As an example of an IEF search and extraction, the laptop computer believed to have been used principally by Tamerlan contained 20,214 internet artifacts, mostly in Russian. These artifacts were reviewed to identify, *e.g.*, those that contained Islamic-related terms, anything to do with explosives, guns, ammunition, and terms related to the political situation in the Caucasus region. Investigation of a single artifact — *e.g.*, a link to a website from browsing history — could prove quite time consuming. Each such link would have to be "clicked" during the review process in order to ascertain the nature of the content underlying the link. In some cases, if the link was no longer active (the particular web page had expired or changed), further research on an internet archive site was necessary. Ultimately, 1,536 artifacts were identified as potentially relevant, of which 753 were unique.[3] Of these unique artifacts, 551 were in Russian, 153

[3] Some of the artifacts were functionally duplicative, for example, multiple visits to the Kavkaz Center home page (a Russian-language news site concerning the Caucasus). While the page likely had different content on each visit, the unique content viewed on each visit cannot now be reconstructed.

in English, 11 in Uzbek, 5 in Arabic, 2 in a combination of Arabic and English, and the rest undefined (*e.g.*, images of conflict in the Caucasus or Middle East that did not have identifiable language content). The process of extracting and reviewing these artifacts required approximately a month of full-time work.

15. **FTK** is a software tool that is used to process all of the files on a computer, with the capability to "bookmark" files for further review or to extract selected files. FTK can be used to view both files existing at the time the computer was forensically copied and also has the capability to "carve" some of the files that were previously deleted or overwritten.[4] Once a computer is processed with FTK, individual files of interest must be identified. While targeted keyword searching of text files is possible, informed browsing is still necessary because the aim is to develop an overall understanding of the computer's principal user. Moreover, text searches cannot be used to narrow the field of relevant images and multimedia files.

16. As an example of an FTK search and extraction, the same laptop computer associated with Tamerlan, referenced above, contained 608,262 total files (actual and carved). It contained 31, 337 text files (7,690 carved) of which, ultimately, just 15 were of some interest and 11 were Islam-related. It also contained 237,076 graphic files (198,775 carved), including everything from family photographs to religious imagery. It

---

[4] Conducting further analysis of a "carved" file can be more time consuming and challenging because file attributes such as the name, date, and original directory location of that file on the computer are absent.

also contained 1,185 multimedia files (audio, video, etc.) of which 74 have been identified as of interest in a review process that is still ongoing.

17. To date, the defense has accomplished substantial work on three of the seven computers produced in discovery: laptops believed to have been principally used by Tamerlan and Dzhokhar, respectively, and a desktop computer apparently shared by multiple Tsarnaev family members at their Cambridge residence. At the same time, much work still remains to be performed on evidence derived from these computers before the defense can move on to focus on others, including devices belonging to other family members and friends of Mr. Tsarnaev.

Data Storage Media

18. Data storage media such as USB thumb drives and external hard drives are examined using FTK, which, as with computers, identifies actual currently-existing files as well as "carved" files.

19. As an example, the external hard drive apparently recovered from one of the Tsarnaevs' vehicles at the Watertown shootout scene contained 46,892 files (15,794 carved) of which 51 are compressed file archives, 2,158 (1,668 carved) are text documents, 21,515 (13, 947 carved) are graphics, and 9,286 are multimedia. Review is ongoing; 76 files have proven to be of interest thus far.

20. To date, the defense has accomplished substantial work on 4 of the 10 data storage devices.

Cellular Phones

21. The government has produced phones in this case either in raw image form (a forensic copy, analogous to the manner in which computers were produced) which is then processed by the defense or in the form of forensic extraction "reports" containing data and other materials taken from the phone.[5]

22. Types of information typically extracted from a phone include call records; phone book, notes, voice notes, voicemail, SMS/MMS text messages, emails, images and multimedia (from internet as well as photos and videos created by the phone itself), web browsing history, and GPS data. Much of the textual and multimedia information is in Russian. As with other devices (computers and media storage), all of this material must be reviewed manually for potential relevance.

23. As an example, the phone of Mr. Tsarnaev's friend, Dias Kadyrbaev (who recently pled guilty to federal charges), is illustrative.

24. Dias' phone contained approximately 13, 000 text messages, most of them in Russian plus a handful using Kazakh phrases. The phone apparently was shared between Dias and his mother, and further review revealed that only about 3,000 messages were actually sent to/from Dias during a couple of months that he had the phone in his possession. After translation, these text messages with accompanying information filled 250 pages of small-print text. These messages provide a unique and valuable glimpse

[5] In several cases the government has produced multiple reports for the same phone, made at different times with different software tools. These reports vary in their contents and completeness such that, as a first step, the defense must create a combined "hybrid" collection of material incorporating elements of each report.

into the life of our client and his peers at UMass Dartmouth, into the family life of Mr. Tsarnaev during times when Dias stayed at the Tsarnaev family home in Cambridge and exchanged texts with his mother about his experiences.

25. Dias' phone also contained approximately 30,000 images. After review, we managed to distill it to 350 images of interest. As with text messages, these depict the interests of Mr. Tsarnaev and his friends over time, their whereabouts, and their associations with others.

26. To date, the defense has accomplished substantial work on 6 of the 13 phones produced.

File Origin and Transfer History

27. In addition to extracting derivative evidence from electronic devices and reviewing that evidence for relevance, additional forensic examination is necessary to conduct on certain files of particular interest in order to try, with available information, to determine the device on which the file originated, the history of file transfer among various seized devices, and the individuals using the relevant devices at the time of creation or transfer. Multiple tools and sources of information must be employed to perform this task; the analysis of a single file in this manner can require one or more full days of work.

Conclusion

28. While the defense has made substantial progress processing and reviewing seized electronic devices, the volume of material is daunting. As noted, several

additional device copies were produced in mid-August 2014 and still more can be expected.

29. Thorough review of all of these devices would easily require as much as an additional year of work. Hiring additional computer forensic examiners would be unlikely to accelerate the process meaningfully because the primary bottleneck is not the raw processing and extraction of data but rather the review of data, much of it in Russian, by members of the defense team with sufficient background knowledge to make reasoned judgments concerning relevance.

Sworn under the pains and penalties of perjury this 29th Day of August, 2014.

/s/ William W. Fick